Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to the Department for Business, Energy and Industrial Strategy consultation *Smart Data: Putting consumers in control of their data and enabling innovation.*

The Information Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation ('GDPR'), the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and the Privacy and Electronic Communications Regulations 2003 ('PECR'). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Commissioner welcomes the opportunity to respond to this consultation, produced by the Department for Business, Energy and Industrial Strategy ('BEIS') regarding its Smart Data review. The Commissioner is supportive of initiatives that provide individuals with control and increased access to the information that organisations hold about them. The Commissioner is also supportive of programmes of work that allow personal data to be utilised in beneficial ways, for both industry and the consumer.

Over a number of years, the ICO has provided advice and guidance to the Government on similar initiatives, such as Open Banking and the Midata programme[1]. We are of the view that establishing and maintaining the trust of the consumer is vital in ensuring the success of these projects and they should continue to be at the heart of the Smart Data review.

As such, in bringing together this response on the Smart Data consultation, the ICO is seeking to ensure individuals make informed decisions about sharing their data, and that the terms of the processing are clear to them. Building consumer trust and confidence should be integral to the development of the Smart Data project.

Data protection is not, and should not be seen, as a barrier to stimulating competition, driving innovation and procuring new business models within the realm of Smart Data. When applied appropriately, the requirements of data

[1] https://ico.org.uk/media/about-the-ico/consultations/2013714/dbeis-energy-midata-ico-response-20170210.pdf

protection law should further enhance the products and services the Smart Data project is looking to encourage.

We have reviewed the consultation paper and identified the points that relate to the privacy of individuals and therefore fall within our remit to respond.

Enabling data driven innovation in consumer markets

1. Do you agree with the proposed objectives and expected benefits of Open Communications? Are there any other benefits or risks that we should consider?

Following the 2018 Consumer Markets Green Paper, the ICO understands the Government's desire to accelerate the development of new data-driven technologies and services[2].

The development of the Smart Data review should ensure personal data is protected appropriately, with sufficient consideration given to interrelated legal frameworks that will be essential for successful adoption of Open Communications.

Firstly, it is important to acknowledge the parallels and crossovers between Smart Data and the GDPR's data portability requirements[3]. Of the 'key features' of Smart Data identified within the review, the concepts of immediate provision of data to third party providers ('TPPs') and the use of application programming interfaces ('APIs') for data sharing relate directly to the GDPR's requirements.

Whilst the Smart Data consultation suggests that the provision of data to TPPs is accelerated from the GDPR requirement of one month, to an immediate transfer of data, appropriate consideration should be given to other principles of the GDPR.

For example, before the data is shared, the data controller should ensure the data is relevant and not excessive, in accordance with the GDPR's data minimisation principle. The processing should also consist of appropriate security measures to maintain the integrity and confidentiality of the data, as required by

[2] https://ico.org.uk/media/about-the-ico/consultation-responses/2019/2614964/ofgem-call-for-evidence-on-consumer-impact.pdf
[3] https://gdpr-info.eu/art-20-gdpr/

the GDPR's security principle.

The decision to base the use of APIs on 'express consent' from the individual should also be given thorough consideration. The GDPR sets a high standard for consent[4] and if it is difficult to obtain or uphold the rights of individuals when relying on it, another lawful basis may be more appropriate. Consent of a GDPR standard should put individuals in control as well as build trust and engagement in the processing activity.

Both of these matters exemplify the need for thorough consideration of the mechanics of such proposals before they are implemented. Whilst there are elements of processing involved in the Smart Data review that are unlikely to result in a high risk to individuals, it is still recommend that a Data Protection Impact Assessment[5] is undertaken for any major project that requires the processing of personal data.

2. What is the most effective approach to implementation to ensure the success of Open Communications in enabling innovation and delivering the best consumer outcomes?

Government should ensure it builds privacy into the development of programmes such as Smart Data and the Open Communications initiative. It is the Commissioner's view that technological development should not be a case of privacy *or* innovation, but privacy *and* innovation[6].

The ICO has engaged with BEIS on a number of data-driven projects both in the developmental stage and in formal consultation regarding smart metering and Midata, as well as initial engagement regarding Smart Data implementation. Throughout, we have maintained that establishing and maintaining consumer trust is of significant importance to such schemes.

With regards to effective implementation of Open Communications, the Commissioner would be broadly supportive of the intention to administer common technical standards, formats and definitions as a way to ensure interoperability. Applying these standards is largely consistent with the data portability requirements outlined in Article 20 of the GDPR. The legislation

[4] https://gdpr-info.eu/recitals/no-32/

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

[6] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/promoting-privacy-with-innovation-within-the-law/

explains that data should be managed in a structured, commonly used and machine-readable format.

Furthermore, Article 29 Working Party guidance[7] on data portability makes strong recommendations that industry stakeholders and trade associations work together to develop a common set of interoperable standards and formats to deliver the requirements of the right to data portability. These recommendations seem consistent with the approaches outlined within the key features of the initiative.

3. In which other markets, outside of the regulated and digital markets, would there be the greatest benefits from Smart Data initiatives? Please explain your reasoning

As outlined in the ICO's response to the Green paper, it is not within the Commissioner's remit to comment on the application of Smart Data to particular sectors or markets, given that the GDPR does not consider within which the concepts of data portability will apply.

Using data and technology to help vulnerable consumers

9. What other actions could the Government or regulators take to support the use of data and innovative services to improve outcomes for vulnerable consumers?

The Commissioner is in agreement with the proposals laid out in the consultation that legislative and regulatory requirements are significant in allowing all individuals access to the benefits and support that can be provided as part of the Smart Data programme. This is particularly true of consumers who have some form of categorisation as 'vulnerable'.

The Commissioner acknowledges that what makes a consumer vulnerable will vary in different circumstances and may often be transient in nature. The ICO is engaged with a range of other regulators and stakeholders in the public, private and third sector to discuss how better outcomes can be achieved for vulnerable customers while respecting their privacy rights.

[7] https://ec.europa.eu/newsroom/document.cfm?doc_id=44099

Whilst data protection law has an important role in setting the legal context within which the Open Communications project will sit, it should not be the defining regulation, given the broad scope of individuals it may affect - particularly within the context of vulnerability. Therefore, other forms of legislation or regulatory direction should be considered alongside the GDPR, as the Smart Data process looks to innovative services and improve outcomes for vulnerable consumers.

The ICO has recently joined the UK Regulators Network ('UKRN') as a full member. As part of the network, we are in a strong position to understand the issues facing similar authorities, recognise comparable projects, and inform future considerations from data protection perspective.

As such, the Commissioner would encourage BEIS to make full use of forums such as the UKRN, to establish how the Smart Data project can be utilised, where appropriate, for consumers identified as vulnerable.

11. How can we ensure that the Smart Data Function improves outcomes for vulnerable consumers? Do we need to consider any further actions?

In the context of Smart Data, clarity around the consents provided by customers – including vulnerable customers – is particularly important. When relying on consent as the basis for processing personal data, the processing should involve choice and control for the individual as to how their data is used. Options being provided to consumers should be granular enough so that they are able to provide consent separately for other specific, distinct purposes.

For example, any forthcoming engagement regarding the 'Vulnerable Consumer Challenge' should draw a clear distinction between processing that is necessary for the fulfilment of the consumer's usual services and any additional processing that is undertaken as part of new initiatives for the project.

Data controllers involved in the initiative must clearly explain to individuals what they are consenting to, in a way they can easily understand. If the request for consent is unclear, cumbersome or difficult to comprehend, then it will be invalid. Even if the new purpose and project is considered 'compatible' with the original purpose, this does not override the need for consent to be specific.

Certainly in the context of vulnerability, there is potential that information will be classed as 'special category data', particularly where the vulnerability relates to the individual's health. As the GDPR identifies this type of data as particularly

sensitive[8], it requires additional safeguards to be applied and consideration as to whether the processing is appropriate.

Protecting consumers and their data

12. Do you agree these protections for when TPPs use Smart Data are needed? Are there others we should consider?

The Commissioner is supportive of the proposed safeguards to protect consumer personal data in the context of TPP access in the Smart Data programme. Legislative and regulatory requirements have a central role in creating a Smart Data programme that consumers will trust and use effectively.

The GDPR requires organisations to take appropriate technical and organisational security measures to prevent the personal data being accidentally or deliberately compromised[9]. The GDPR does not specifically define what security measures should be in place, but requires a level of security that is appropriate for the risks that the processing presents. The appropriate measures will depend on the circumstances of the processing and the risks it presents to both the data subject and data controller.

14. What are the advantages and risks of introducing a cross-sectoral general authorisation regime for TPPs?

In practice, when considering 'appropriate technical and organisational measures' the GDPR allows organisations to take into account the costs of implementation of the project, as well as the nature, scope, context and purposes of processing. Risks must be measured considering the likelihood of occurrence and severity of impact on the rights and freedoms of individuals. An accredited approach to third-party access that builds on the existing requirements of the GDPR appears appropriate in this context.

However, as explored within the consultation, applying an accredited approach to a myriad of TTPs within a range of sectors could prove problematic when it comes to effective operation of the Smart Data initiative. It is important that the programme is able to balance functionality for both consumers and TPPs whilst maintaining appropriate technical and organisational security standards.

[8] https://gdpr-info.eu/recitals/no-51/
[9] https://gdpr-info.eu/art-32-gdpr/

The Smart Data consultation appears to address this, proposing a unified cross-sectoral accreditation process backed by proposals to legislate for strengthened enforcement powers of regulators and the suggested cross-sectoral authorisation regime.

As considered earlier in this consultation response, it is important that suitable fair processing information is provided before data is gathered, and the consents provided by consumers are appropriate for the above proposals.

As part of the GDPR's transparency and documentation requirements, a appropriate audit trail mechanism to inform users about who has accessed their data and when should be compiled by data controllers. Processing should also acknowledge the GDPR's data minimisation requirements, ensuring TPPs are only granted access to personal data that is strictly necessary for the specified processing.

Ultimately, the ICO advocates a 'privacy by design' approach to data processing, which mirrors the requirements of Article 25 of the GDPR. BEIS and any data controller involved in the Smart Data initiative will need to ensure privacy risks are identified from the outset of the project, ensuring data privacy is built into the programme and not 'bolted on' at a later stage.